Electronic Signatures

Electronic filings

presented by: Office of the Secretary of State
Russ Savage, Electronic Transactions Liaison
Michael Totherow, Chief Information Officer

Government Paperwork Elimination Act (GPEA)

Over 100 federal agencies, boards and commissions have reviewed and streamlined their reports - 7,741 reports have been reviewed, reports having an estimated 66 *billion* annual responses.

We are all moving from paper filings to electronic filings. This allows us to simplify the processes of creating, handling and dispersing the inevitable forms used in government. In fact many forms can be eliminated as electronic distribution allows an initial form to be directly “parsed” into the subsequent “child” forms that often move parts of the original to other, appropriate departments or agencies (since various procedures require registration or notice of another party or agency).

Technology Neutral (aka vague about <u>how</u> you do it)

44-7001. Definitions (UETA - Uniform Electronic Transactions Act)
7. "*Electronic Record*" means a record that is created, generated, sent, communicated, received or stored by electronic means.
8. "*Electronic Signature*" means an electronic sound, symbol or process that is attached to or logically associated with a record and that is executed or adopted by an individual with the intent to sign the record.
14. "*Security Procedure*" means a procedure that is employed to verify that an electronic signature, record or performance is that of a specific person or to detect changes or errors in the information in an electronic record. Security procedure includes a procedure that requires the use of algorithms or other codes, identifying words or numbers or encryption, callback or other acknowledgment procedures.

SEC. 106. DEFINITIONS (E-SIGN)
For purposes of this title:
(4) *Electronic Record* —The term ‘‘electronic record’’ means a contract or other record created, generated, sent, communicated, received, or stored by electronic means.
(5) *Electronic Signature* —The term ‘‘electronic signature’’ means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.

Signature Law Summary

- **Arizona A.R.S. 41-132 (by/with state agencies)**
  very specific criteria for linking signature to person (& security of document)

- **Arizona Electronic Transaction Act (AETA/UETA - in-state commerce)**
  focus on sending/receiving the record
  "The effect of an electronic record or electronic signature attributed to a person .... is **determined from the context and surrounding circumstances** at the time of its creation, execution, or adoption, including the parties' agreement, if any, and otherwise as provided by law."

- **Federal Electronic Signatures in Global and National Commerce Act (E-SIGN - interstate and international commerce)**
  signed record "**remains accessible to all persons who are entitled to access** by statute, regulation, or rule of law, for the period required by such statute, regulation, or rule of law, in a form that is capable of being accurately reproduced for later reference, whether by transmission, printing, or otherwise."

E-SIGN

SEC. 104. Applicability To Federal And State Governments.

(b) Preservation Of Existing Rulemaking Authority.—

(2)(C) such agency finds, in connection with the issuance of such regulation, order, or guidance, that—

(i) there is a substantial justification for the regulation, order, or guidance;

(ii) the methods selected to carry out that purpose—

(I) are substantially equivalent to the requirements imposed on records that are not electronic records; and

(II) will not impose unreasonable costs on the acceptance and use of electronic records; and

(iii) *the methods selected to carry out that purpose do not require, or accord greater legal status or effect to, the implementation or application of a specific technology or technical specification for performing the functions of creating, storing, generating, receiving, communicating, or authenticating electronic records or electronic signatures.*

Required Technology Neutrality

E-SIGN

SEC. 104. Applicability To Federal And State Governments.

(3) Performance Standards.—

(A) Accuracy, Record Integrity, Accessibility.—

Notwithstanding paragraph (2)(C)(iii), a Federal regulatory agency or State regulatory agency may interpret section 101(d) to **specify performance standards to assure accuracy, record integrity, and accessibility of records that are required to be retained.** Such performance standards may be specified in a manner that imposes a requirement in violation of paragraph (2)(C)(iii) if the requirement

(i) serves an important governmental objective; and

(ii) is substantially related to the achievement of that objective.

Nothing in this paragraph shall be construed to grant any Federal regulatory agency or State regulatory agency authority to require use of a particular type of software or hardware in order to comply with section 101(d).

So what? Consider the lowly car rental contract.

How do we assure accessibility by all parties?

Interoperability requires common document and signing standards across agencies and jurisdictions

Documents may be "self-documenting" or "system documented records" - we'll need a range of standards.

"This initial study led to a detailed description of the electronic record. We determined that **an electronic record had to be a fully self-documenting object.** We chose to describe these objects in eXtensible Markup Language (XML), a text based standard. We determined that an electronic record was made up of one or more documents, contextual information relating this record with other records, and evidential integrity checks."

Victorian Electronic Records Strategy Final Report

One Interoperability example is LegalXML which is establishing court document standards.

http://www.legalxml.org/

Example of System Documented Records

What is EDI?

Electronic Data Interchange (EDI) is the computer-to-computer exchange of business-related documents in a structured, machine processable format. These documents may be purchase orders, invoices, payment remittances and shipping notices between the State of Ohio and its "trading partners." A trading partner, in EDI parlance, is a supplier, customer, subsidiary or any other organization with which the state of Ohio does business. EDI differs from e-mail and fax. Although both of these methods of transferring documents are electronic, both are unstructured and free-form in the way they are presented. This means that information received via e-mail or fax must be rekeyed and reinterpreted before it can be processed by a computer application. EDI, on the other hand, requires that the information be organized in a structured format which can be easily interpreted and processed by a computer application.

Ohio - *http://www.state.oh.us/ecedi/welcome.htm*

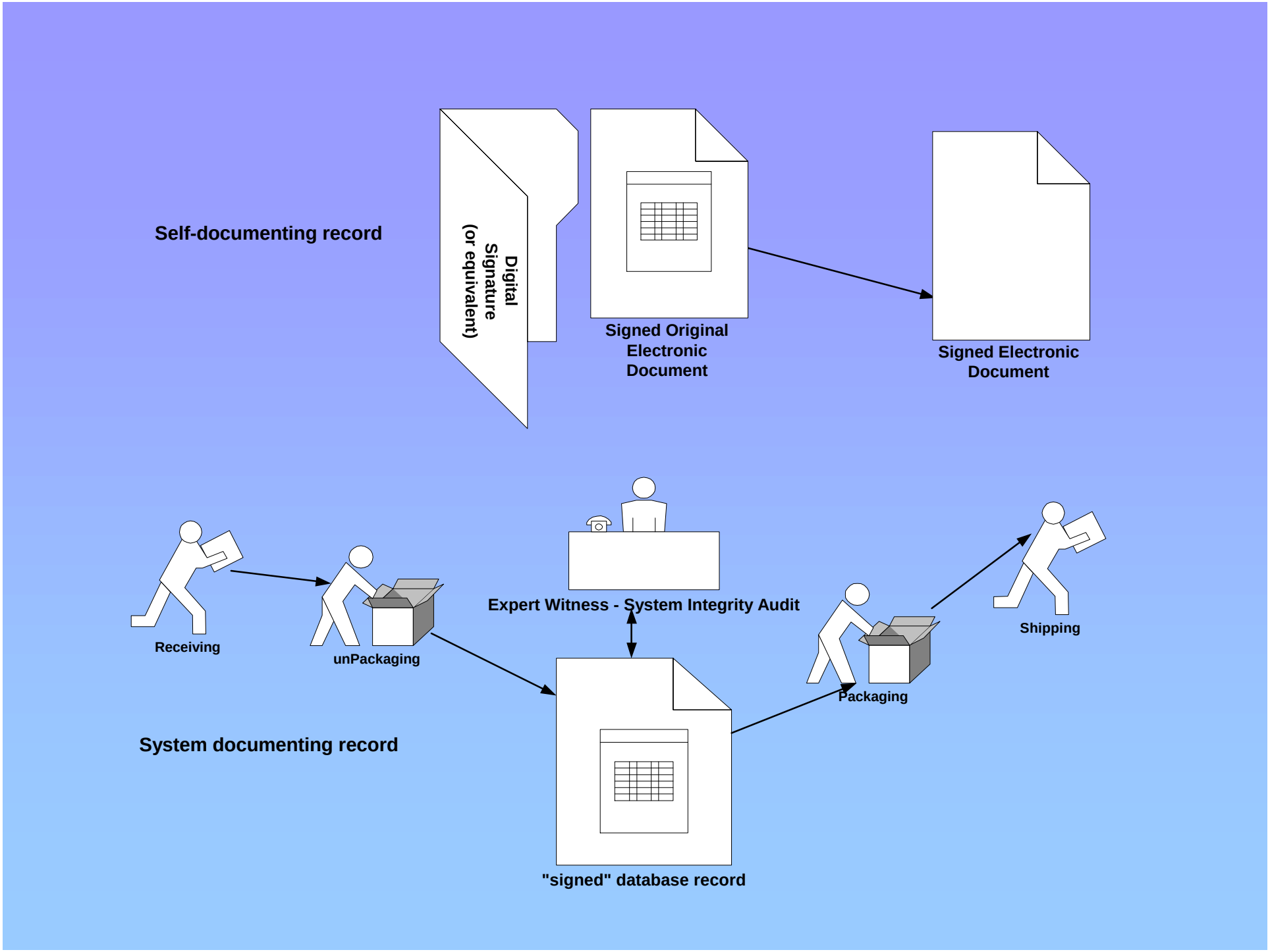
Example of System Documented Records

How EDI Works - Briefly (Ohio continued)

EDI involves taking a standard computer flat file and reformatting the file into a structured EDI format. This format complies with specific industry standards. This reformatting process is performed by a specialized software program called an EDI translator.

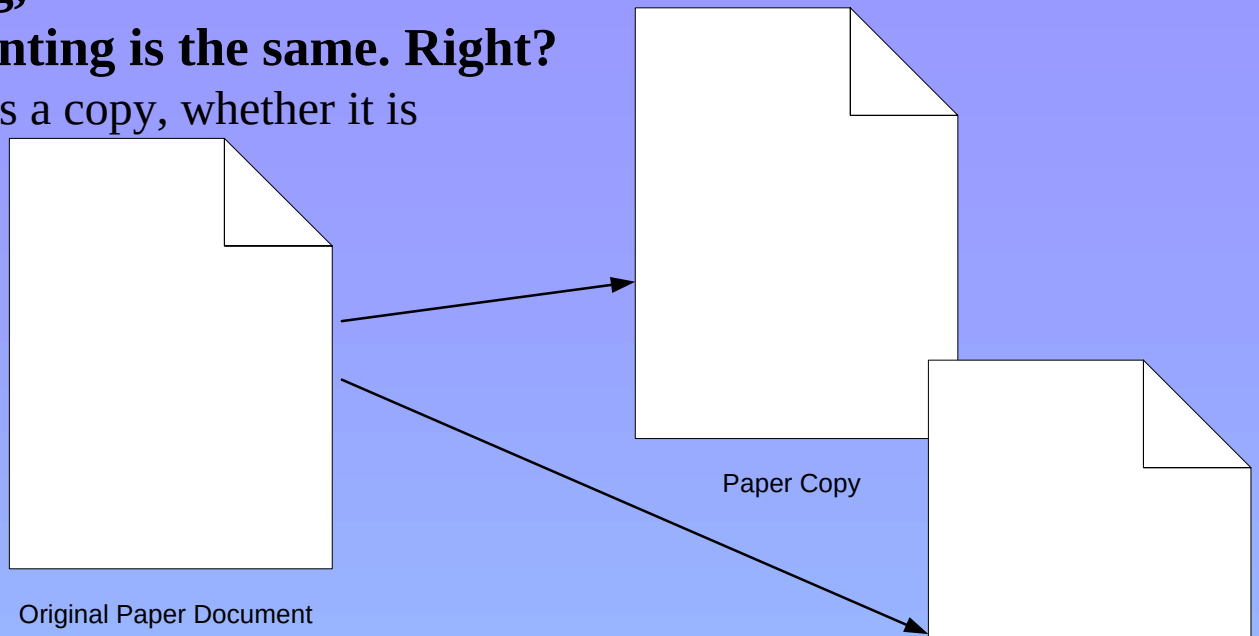
Once the file has been put into a structured format, it is transmitted over telephone lines to a third party network. The third-party network called a Value Added Network (VAN) provides a service much like a post office. The VAN receives the transmitted documents and places these documents into an electronic mailbox for the receiving party to pick up. By dialing into the network, the receiving party can access its mailbox and retrieve the transmitted documents.

Once the electronic documents have been accessed by the receiving party, the documents once again can be processed through an EDI translator. The translator takes the documents, which are still in EDI format, and translates them into a standard computer flat file. This flat file then can be formatted into a report and printed out or sent directly into a company's computer application for processing.

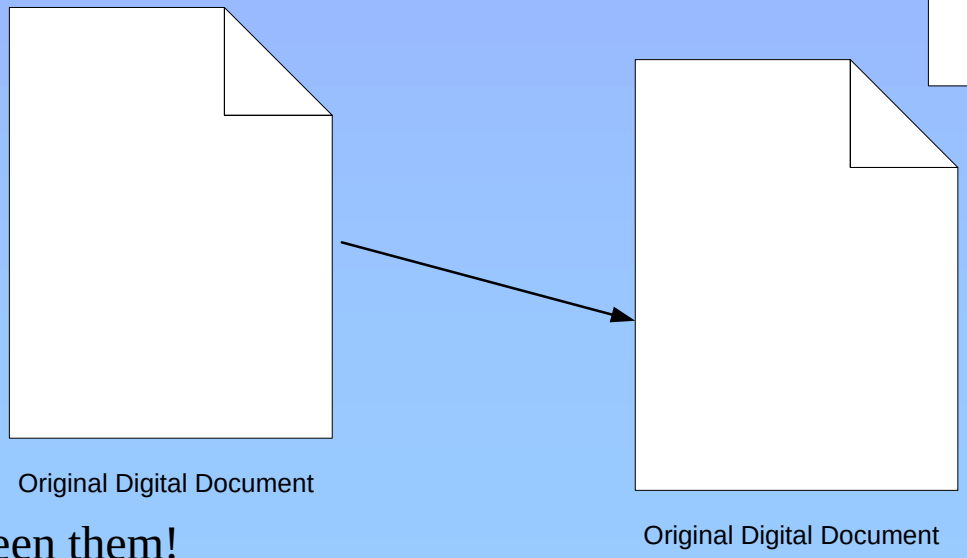

Self-documenting record
Digital Signature (or equivalent)
Signed Original Electronic Document
Signed Electronic Document
Receiving
unPackaging
Expert Witness - System Integrity Audit
Packaging
Shipping
System documenting record
"signed" database record

Paper is self documenting,
so electronic self-documenting is the same. Right?

A copy of a paper document is a copy, whether it is another paper document or a digital image.



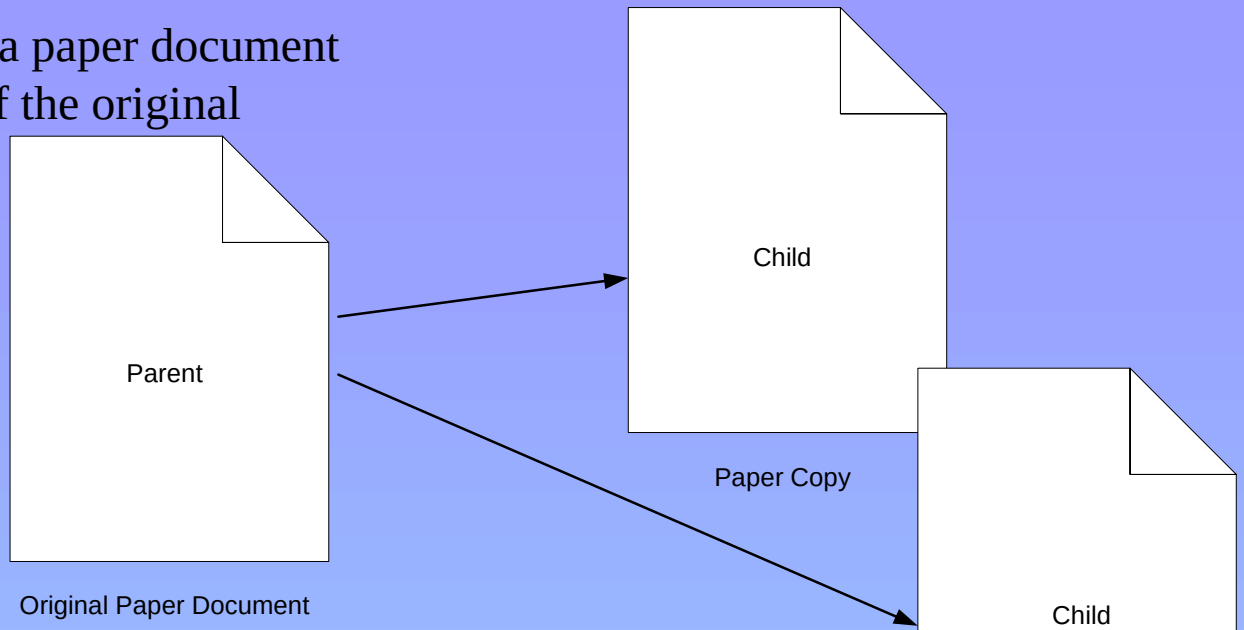
It is possible to send an original digital document to someone - while you keep the original of it.



There is *no* difference between them!

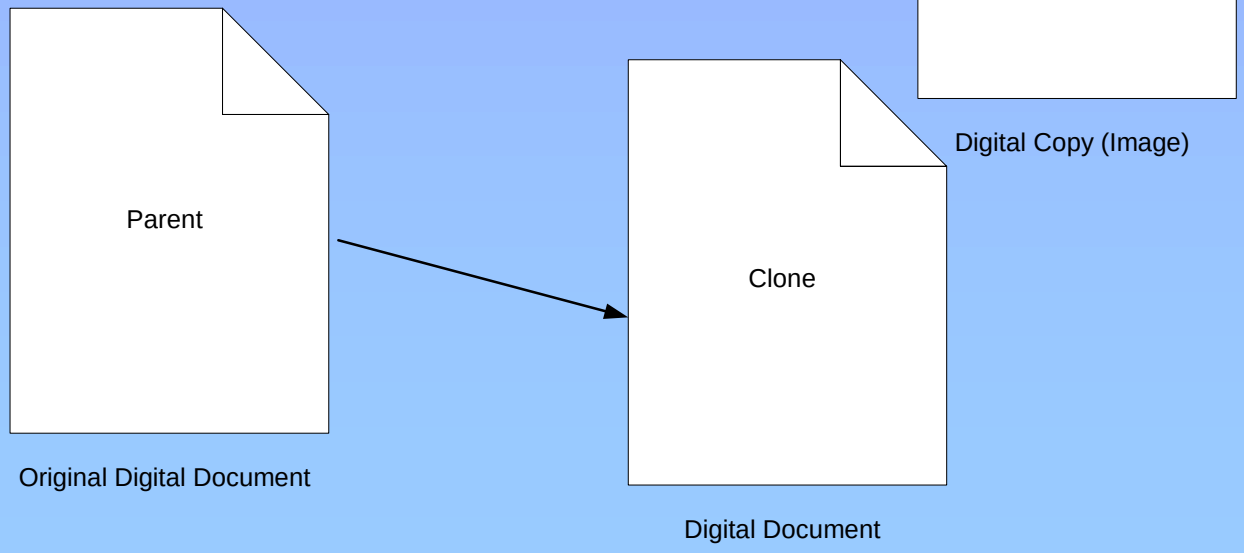
Self-Documenting Records

The validity of a copy of a paper document depends on the validity of the original (and that the copy hasn't been altered).



The validity of a digital document depends on the tests it can pass - including whether it has been altered.

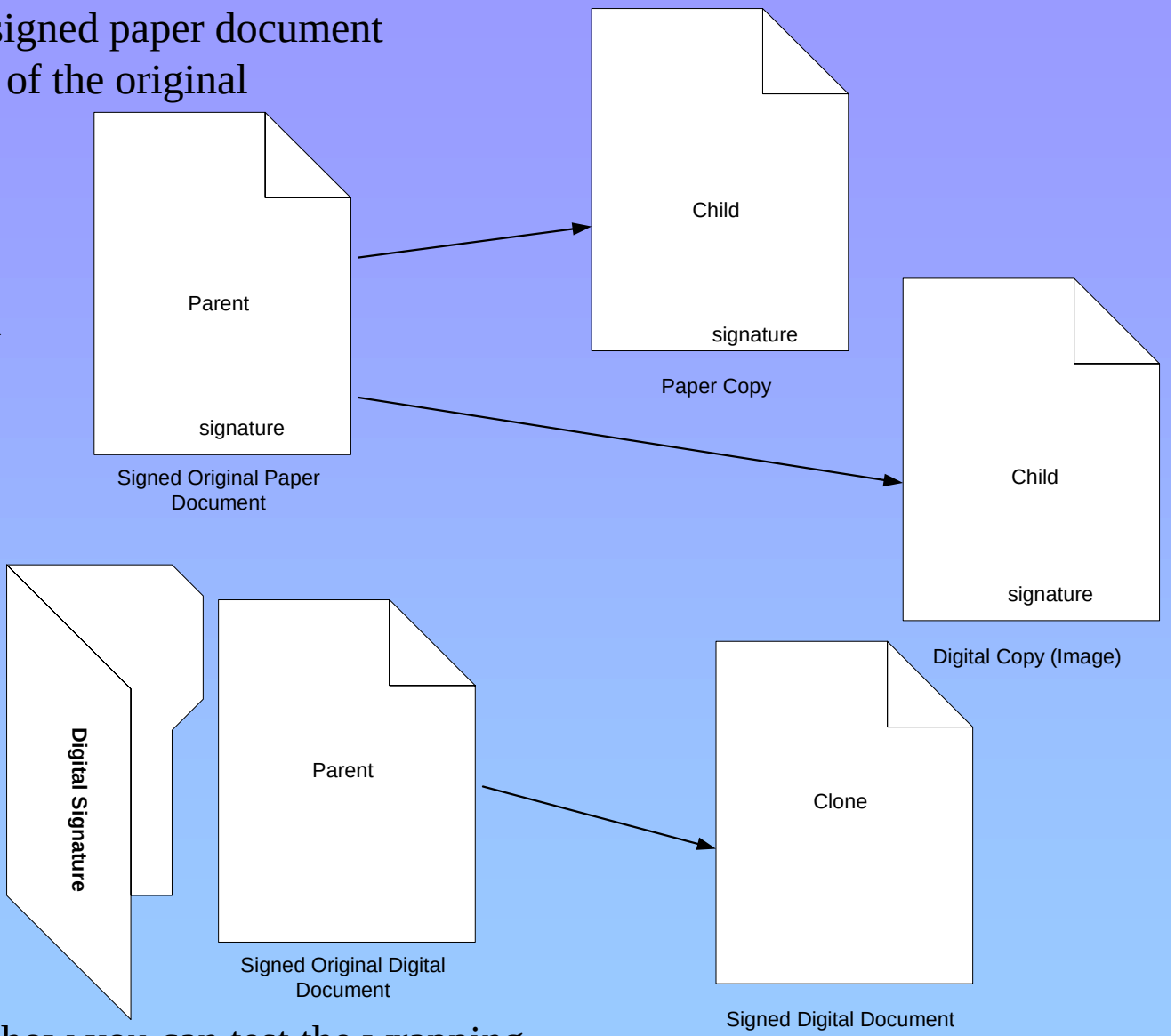
Since there is no copy, only a clone, those tests apply to the clone as well.



Self-Documenting Records

The validity of a copy of a signed paper document still depends on the validity of the original (and that the copy hasn't been altered).

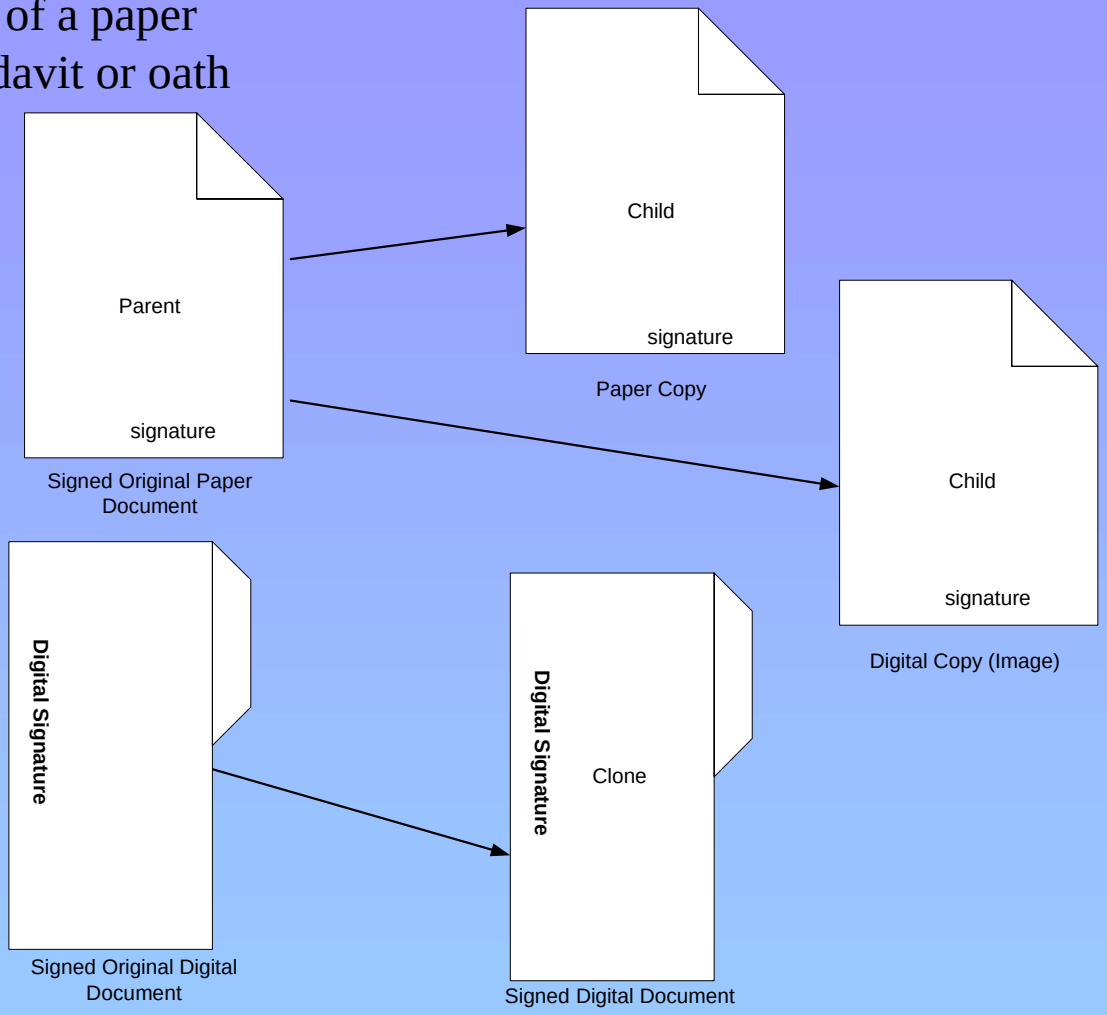
There is the extra complication that you could sign a copy which would add "legal standing" to the copy.
You could even make it a clone!



A digital signature wraps the document. The validity of the document depends on how you can test the wrapping such that its contents were not altered.

Self-Documenting Records

Keeping a “legal” digital image of a paper original usually requires an affidavit or oath that it is a true, unaltered copy.

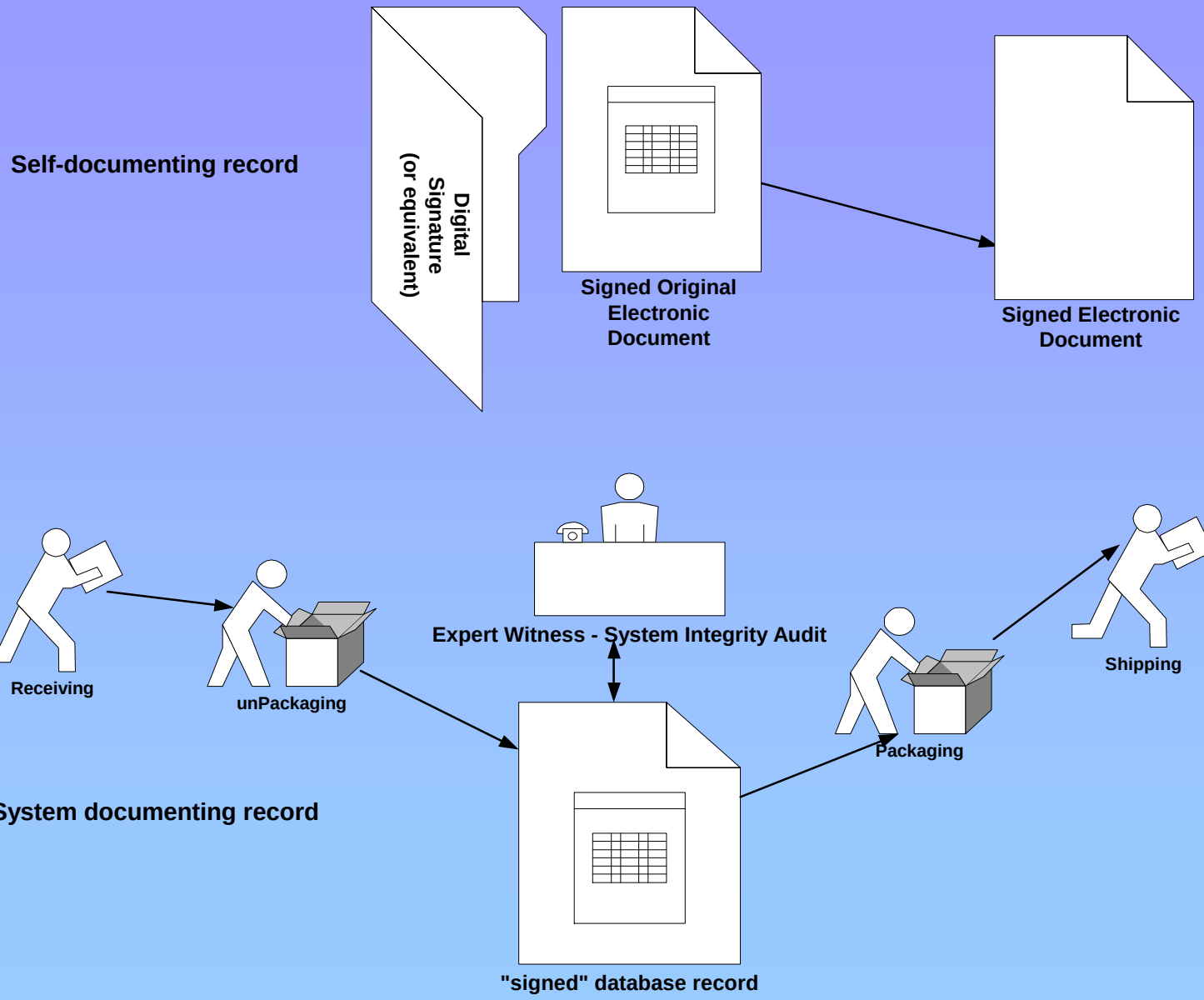


Keeping a “legal” digital document requires being able, over time, to test the signature’s validity and keeping the wrapped contents readable.

Records Management Guidance for Implementing Electronic Signature Technologies

- Electronic signature records need to be retained based on their operational needs and perceptions of risk.
- If an electronically signed record needs to be preserved, whether for a finite period of time or permanently, then its trustworthiness over time needs to be assured.
- Use of a records retention schedule needs to include
    - designating the disposition authority to dispose of records
    - the means to dispose of records at the end of the scheduled retention

If an electronically signed record needs to be preserved, then its trustworthiness over time needs to be assured.



Trustworthy Records

Reliability - record content can be trusted as a full and accurate representation of the transactions, activities, or facts to which it attests and can be depended upon in the course of subsequent transactions or activities.

Authenticity - a record proven to be what it purports to be and to have been created or sent by the person who purports to have created and sent it.

Usability - a record that can be located, retrieved, presented, and interpreted. In any subsequent retrieval and use, the record should be capable of being directly connected to the business activity or transaction which produced it. It should be possible to identify a record within the context of broader business activities and functions. The links between records which document a sequence of activities should be maintained. These contextual linkages of records should carry the information needed for an understanding of the transaction that created and used them.

Trustworthy Records (cont.)

Integrity - a record being complete and unaltered.

- protect record against alteration without appropriate permission.

- records management policies and procedures should specify
  - what, if any, additions or annotations may be made to a record after it is created,
  - under what circumstances additions or annotations may be authorized, and
  - who is authorized to make them.

- Any authorized annotation or addition to a record made after it is complete should be explicitly indicated as annotations or additions.

- structural integrity of a record - the structure of a record should remain physically or logically intact - its physical and logical format and the relationships between the data elements comprising the record. Failure to maintain the record's structural integrity may impair its reliability and authenticity.

Preserving Trustworthy Records

For a record to remain reliable, authentic, with its integrity maintained, and useable over the record life cycle, it is necessary to preserve its content, context, and sometimes its structure.

A trustworthy record preserves the actual content of the record itself and information about the record that relates to the context in which it was created and used (e.g. formatting of presentation).

Specific contextual information will vary depending upon the business, legal, and regulatory requirements of the business.

It also may be necessary to preserve the structure or arrangement of its parts. Failure to preserve the structure of the record will impair its structural integrity. That may undermine the record's reliability and authenticity (e.g. Linking the parts of the record together - presentation organizational instructions such as what text with what graphic).

Preserving Trustworthy Records

*Content**

- The electronic signature or signatures in a record are part of the content.
- They indicate who signed a record and whether that person approved the content of the record.
- Multiple signatures can indicate initial approval and subsequent concurrency.
- Signatures are often accompanied by dates and other identifiers such as organization or title.
- All of this is part of the content of the record and needs to be preserved.
- Lack of this information seriously affects a document's reliability and authenticity.

* text largely from
"Records Management Guidance for Agencies Implementing Electronic Signature Technologies"
National Archives and Records Administration, Oct. 18, 2000

Preserving Trustworthy Records

*Context**

- Some electronic signature technologies rely on individual identifiers that are not embedded in the content of the record, trust paths, and other means to create and verify the validity of an electronic signature. This information is outside of the *content* of the record, but is nevertheless important to the *context* of the record as it provides additional evidence to support the reliability and authenticity of the record.
- Lack of these contextual records seriously affects one's ability to verify the validity of the signed content.

* text largely from
"Records Management Guidance for Agencies Implementing Electronic Signature Technologies"
National Archives and Records Administration, Oct. 18, 2000

Preserving Trustworthy Records

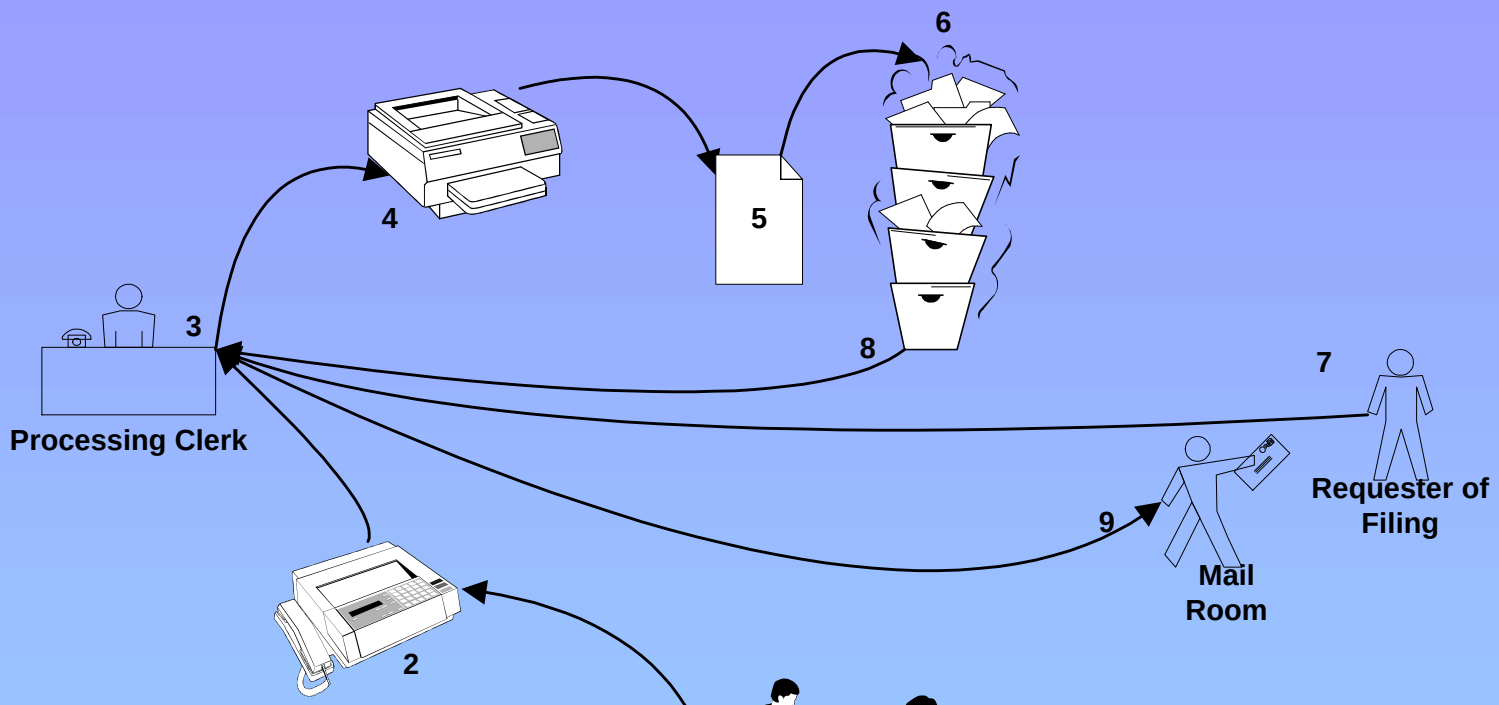
*Structure**

- Preserving the structure of a record means its physical and logical format and the relationships between the data elements comprising the record remain physically and logically intact.
- It may be necessary to maintain the structure of the electronic signature. In that case it is necessary to retain the hardware and software that created the signature (e.g., chips or encryption algorithms) so that the complete record could be revalidated at a later time as needed.

* text largely from
"Records Management Guidance for Agencies Implementing Electronic Signature Technologies"
National Archives and Records Administration, Oct. 18, 2000

Preserving Trustworthy Records

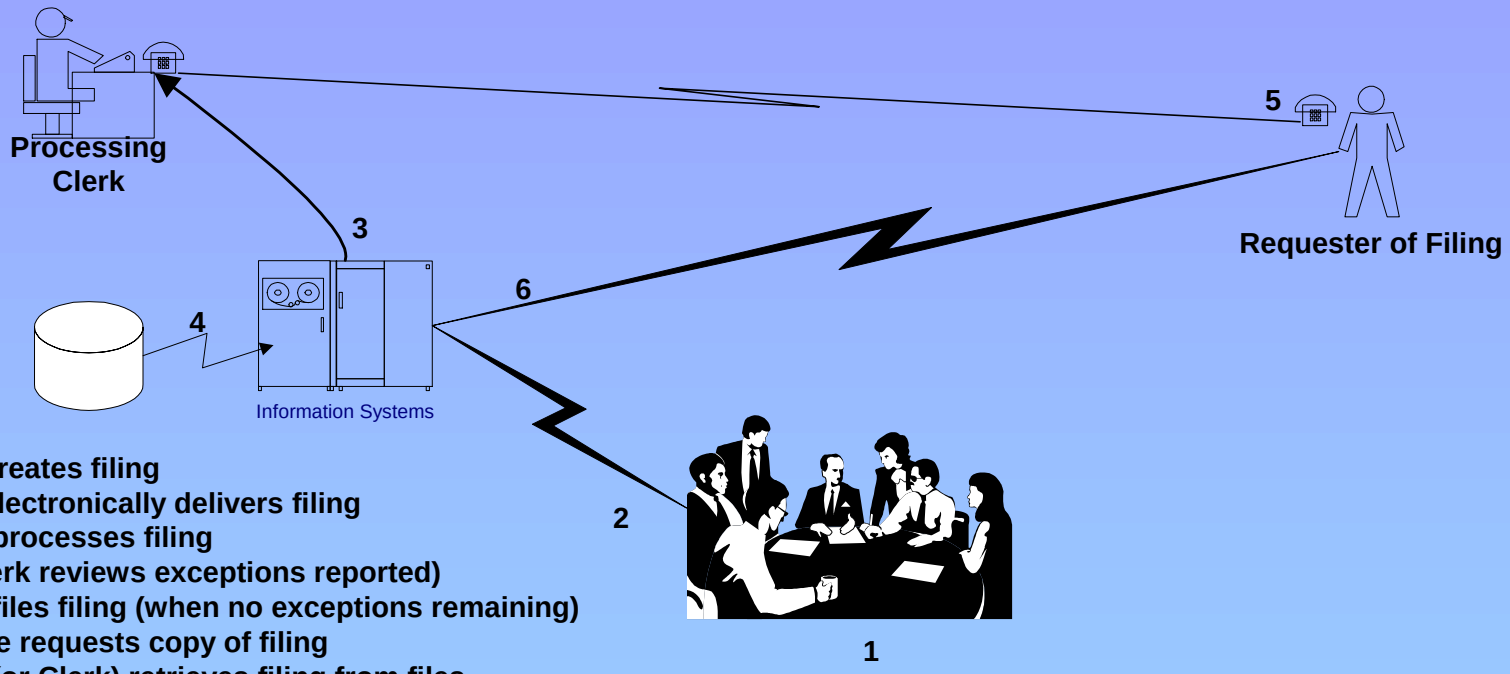
Processing a filing and creating a certified copy



1. Patron creates filing
2. Patron faxes/delivers filing
3. Clerk processes filing
4. & 5. Clerk makes copies (if necessary)
6. Clerk files filing
7. Someone requests copy of filing
8. Clerk retrieves filing from files, makes copy, certifies copy
9. Certified copy if mailed/pickedup

Preserving Trustworthy Records

Processing a filing and creating a certified copy



1. Patron creates filing
2. Patron electronically delivers filing
3. System processes filing
   (and Clerk reviews exceptions reported)
4. System files filing (when no exceptions remaining)
5. Someone requests copy of filing
6. System (or Clerk) retrieves filing from files,
   transmits a certified copy

Preserving Trustworthy Records

All of the checks and balances (the evidentiary proof) in the paper world will need to be mimicked in the electronic world - the clerk stamps the filing on receipt, files a self-documenting, signed original paper record, and, when requested, a copy is stamped as a certified copy.

Some form of technical “non-repudiation” services must be implemented to protect reliability, authenticity, integrity and usability.

Essential elements:

- Evidence of the origin of the message
- Evidence of sent
- Evidence of receipt
- Timestamp as needed of origin, sent, receipt
- Long-term storage of evidence
- Designated adjudicator of prospective disputes

Remember that you’re not alone, others need access to those documents and records. And they need assurance that you protected the reliability, authenticity, integrity and usability of those records..